International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Ponzi Scheme Detection and Identification in Cryptocurrency-Based Scams using Machine Learning Techniques

Vishal Sharma[1], Dr. Ankush Shrivastava[2]

[1]Research Scholar, Faculty of Engineering and Technology, RKDF University, Bhopal
[2]Associate Professor, Faculty of Engineering and Technology, RKDF University, Bhopal

Abstract
The rapid expansion of cryptocurrency markets has provided fertile ground for financial fraud, particularly Ponzi schemes that promise high returns to early investors using funds from later participants. The pseudonymous and decentralized nature of blockchain transactions makes manual detection infeasible at scale. This research work proposes a machine learning (ML) framework for automated detection and identification of Ponzi schemes in cryptocurrency networks. The complete transaction ecosystem is modeled as a directed temporal graph and extracts some structural and dynamic features, which include transaction velocity, early flow ratio, burstiness, and network centrality. An XGBoost ensemble classifier is trained on a simulated dataset (5% Ponzi, 95% normal) and achieves an accuracy of 98.1%, a precision of 96.3%, a recall of 95.7%, an F_1-score of 96.0%, and an AUC-ROC of 99.4%, which outperforms random forest, SVM, and logistic regression baselines. The SHAP analysis identifies transaction velocity and early flow ratio as the most influential features. The proposed framework offers an interpretable, scalable, and highly accurate solution for real-time cryptocurrency fraud monitoring, with potential integration into blockchain surveillance systems.

Keywords: Ponzi Scheme Detection, Cryptocurrency Fraud, Machine Learning, XGBoost, Blockchain Forensics, Transaction Graph Analysis, SHAP Interpretability, Ethereum, Bitcoin.

1. Introduction

The swift increase of cryptocurrencies has drastically changed how transactions are conducted by offering decentralization, anonymity, and borderless transfer (Naysary and Tarazi, 2024; Chen, 2025) [1, 2]. Unfortunately, these same properties have attracted malicious coders who have used the lack of regulations and traceability to commit fraud in the financial arena. Of the most damaging schemes within the cryptocurrency arena are Ponzi schemes, which are basically fraudulent investment operations that pay off investors using the capital of new investors, rather than from actual profit made from an investment (Wilkins *et al.*, 2012; Artzrouni, 2019) [3, 4]. The conventional Ponzi schemes can generally be detected before being identified and ultimately collapse due to legal and regulatory measures, while cryptocurrency schemes may grow to large scales and cause a significant financial impact (Mukherjee *et al.*, 2022; Lee and Keathley, 2022; Boyle and Peng, 2025; Scharfman, 2025) [5-8].

There are worldwide huge numbers of cryptocurrency-related scams, including Ponzi schemes, that result in economic and financial losses. High-profile cases of scams underscore the urgent requirements for automated, scalable, and accurate detection methods (Bosley and Knorr, 2018; Rafik *et al.*, 2023; Song and Kong, 2025; Sotes *et al.*, 2026) [9-12]. The conventional manual auditing and post-collapse forensic analysis are insufficient given the sheer volume of transactions and the speed at which new smart contracts and addresses are created (Yao *et al.*, 2024; J.J. *et al.*, 2024) [13, 14].

Machine learning (ML) generally offers a promising solution by patterns learning techniques from historical transaction data to identify the suspicious behaviors that indicate Ponzi operations (Ibba *et al.*, 2021; Krishnan *et al.*, 2023; Castro Severiche *et al.*, 2025) [15-17]. Several research projects have applied classical ML models such as random forest and support vector machine (SVM) and deep learning approaches such as graph neural networks (GNN) and long short-term memory (LSTM) to detect Ponzi schemes on Bitcoin and Ethereum networks (Jeleskovic, 2024; Kimber *et al.*, 2025) [18, 19]. However, existing methods suffer from three main limitations:

1. They often rely on a narrow set of features, which has missing temporal dynamics and subtle structural anomalies.
2. They lack interpretability, which is critical for financial investigations,
3. They do not incorporate the fundamental economic consistency condition of Ponzi schemes, the net outflow of funds from the scheme is negative for participants as a whole.

To address these research gaps, this research work proposes a novel ML framework for Ponzi scheme detection and identification in cryptocurrency networks.

The remainder of this paper is organized as follows. Section 2 reviews related work on ML-based fraud detection in cryptocurrencies. Section 3 presents the system model with mathematical formulation. Section 4 describes the proposed methodology, including data preprocessing, feature engineering, and the XGBoost classifier. Section 5 details the simulation setup and presents the experimental results and discusses the findings and limitations. Finally, Section 6 concludes the paper and outlines future research directions.

2. Related Work

The increasing prevalence of recent Ponzi schemes in cryptocurrencies also inspired a vast amount of research on applying ML techniques for Ponzi scheme detection and identification. This section provides a survey of key contributions and methodologies and highlights the foundational research that basically informs this work.

A significant contribution in a study conducted by Luo *et al.* (2024) [20] proposed research on AI-driven fraud detection in decentralized finance (DeFi) in the project life cycle, which basically correlates fraud types with DeFi project phases and evaluates AI techniques. This research suggests that tree-based and graph-based models outperform other models in different detection tasks. Feng *et al.* (2024) [21] proposed a novel interpretable ML system, “IDPonzi,” for the detection of smart contract Ponzi schemes in blockchain. By preprocessing data and conducting smart contract opcode analysis, as well as applying SHAP for explainability, their model can improve both detection accuracy and interpretability of the Ponzi schemes. The model has already outperformed traditional methods on three metrics with 99% precision, 85% recall, and 92% F_1-score.

Onu *et al.* (2023) [22] proposed an ML-based method for early detection of Ethereum Ponzi schemes. Using more than 20,000 transaction data and employing a random forest model, their methods reach a high accuracy (94%) while reducing the number of features to be detected from 70 to 10, providing an efficient and precise fraud detection method. Kumar *et al.* (2026) [23] reviewed ML and AI techniques that are mainly used to detect Ponzi schemes on Bitcoin and Ethereum. They summarized existing datasets, features, and detection methods and provided a comprehensive overview of research in the detection of smart Ponzi schemes. Wang *et al.* (2026) [24] proposed "LIGHTPONZI," a lightweight multimodal system to detect Ethereum Ponzi schemes using transaction, code structure, and text features. They achieved high accuracy (0.911 F_1 score) with fast processing, which enables an efficient real-time fraud detection system.

Chen *et al.* (2026) [25] proposed "PonziHunter," which detects the Ethereum Ponzi contracts by converting the bytecode into graph-based representations of control flow and state logic. It improved accuracy, robustness, and generalization over the existing methods and discovered previously unknown Ponzi schemes. Liao *et al.* (2026) [26] presented an explainable ML model to detect blockchain Ponzi schemes using transaction network features and ensemble learning. They achieved very high accuracy and applied SHAP analysis to reveal characteristic fraudulent transaction and network behaviors. Cao *et al.* (2025) [27] proposed "MFDPonzi," a model that detects Ethereum Ponzi contracts using multiple features from smart contract execution and code. This model enables early detection without transaction data and presents improved performance over existing methods.

Wu *et al.* (2026) [28] proposed "HyperDet," a system that improves Ethereum Ponzi detection by using hypergraphs to model multi-party transactions instead of simple pairwise graphs, which leads to better accuracy than traditional graph-based methods. Liu *et al.* (2026) [29] proposed a method for early detection of Ponzi schemes in smart contracts by building a multi-dimensional transaction graph from opcode control flow, cross-contract dependencies, and transaction semantics. Using static analysis and transfer API features, it captures behavioral and fund-flow patterns to improve accuracy and efficiency in identifying complex Ponzi contracts before deployment.

Jiang and Tsai (2025) [30] introduced "DGAD-SPS," an approach that uses a self-supervised directed graph neural network to detect Ethereum Ponzi schemes. It models transactions as directed graphs to capture asymmetric fund flows and treats detection as an anomaly detection problem rather than simple classification. Jin *et al.* (2022) [31] proposed a method called "HFAug," which is basically a feature augmentation module to improve Ethereum Ponzi scheme detection. It enhances existing graph-based methods by capturing heterogeneous account behaviors using a meta-path-based auxiliary graph and transfers this information to standard transaction graphs. Jin *et al.* (2024) [32] proposed another method, "TMFAug," which is a plug-and-play module for Ethereum Ponzi scheme detection. It basically enhances graph-based models by incorporating time-aware heterogeneous transaction patterns. Unlike other existing methods that ignore temporal dynamics or oversimplify graphs, TMFAug captures realistic metapath-based behaviors over time.

Wen *et al.* (2025) [33] proposed an approach "PonziLens+," which is a visual analytics system to identify the smart Ponzi schemes in blockchain contracts. It mainly extracts meaningful execution behaviors from smart contract bytecode and presents them through interactive visual modules to reveal potential fraud patterns. Yang *et al.* (2026) [34] proposed "CASPER," which is a contrastive learning framework for detecting smart Ponzi schemes in blockchain smart contracts. Unlike conventional supervised deep learning methods that require large labeled datasets, CASPER basically learns useful

representations from mostly unlabeled data, which significantly reduces the reliance on costly annotations. Pennella *et al.* (2025) [35] proposed "X-SPIDE," an explainable ML pipeline to detect Ponzi schemes on Ethereum. Unlike other methods that focused mainly on accuracy, it emphasizes interpretability by identifying the key features and explains how they influence classification decisions.

Research Gap

While significant progress can be observed in the existing literature, there are several gaps remain. The most of methods focus exclusively on either transaction-based or code-based features, these basically rarely on integrating both. The temporal transaction dynamics is critical to capture the life-cycle behavior of Ponzi schemes, it remain underexplored beyond a few recent studies. The ensemble methods like XGBoost, despite their proven efficacy, have not been systematically combined with comprehensive feature engineering tailored to Ponzi-specific behavioral patterns. Some approaches incorporate the mathematical consistency conditions inherent to Ponzi schemes such as net negative sum of profits as post-processing verification. This research work addresses these gaps by proposing an XGBoost-based framework that integrates many temporal-structural features, SHAP-based interpretability, and a Ponzi consistency verification condition.

3. System Model

The cryptocurrency transaction network can be modeled as a directed temporal graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{T}, \mathcal{W})$, where, $\mathcal{V} = \{v_1, v_2, \dots, v_n\}$ denotes the set of unique addresses (wallets) involved in transactions, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ represents directed payment edges, here, an edge $e = (v_i, v_j)$ indicates a transfer of cryptocurrency from v_i to v_j, $\mathcal{T}: \mathcal{E} \to \mathbb{R}^+$ assigns a timestamp t_e to each transaction, and $\mathcal{W}: \mathcal{E} \to \mathbb{R}^+$ assigns a transaction amount w_e.

A Ponzi scheme embedded in this graph is characterised by a set of addresses $\mathcal{V}_P \subset \mathcal{V}$ that exhibit a specific flow pattern: early investors receive payouts funded by later investors' contributions, which creates an unsustainable dependency. Let $\mathcal{V}_L \subset \mathcal{V}_P$ be the addresses of known promoters and $\mathcal{V}_I$ the set of ordinary participants. The scheme promises a high return r over a short period Δt. The cash flow for an investor v_i is defined as:

$$C(v_i) = \sum_{e \in \text{in}(v_i)} w_e - \sum_{e \in \text{out}(v_i)} w_e \tag{1}$$

where $\text{in}(v_i)$ and $\text{out}(v_i)$ denotes incoming and outgoing transactions respectively of v_i. A positive $C(v_i)$ indicates net profit.

A "Ponzi Score" $s(v_i)$ can be defineed for each address based on temporal structural features as:

$$s(v_i) = \sigma\left(\beta_0 + \sum_{k=1}^{K} \beta_k \, \phi_k(v_i)\right) \tag{2}$$

where $\phi_k(v_i)$ denotes K engineered features such as in-degree, out-degree, transaction velocity, centrality, and early-late flow ratio, β_k denotes the learned weights, and $\sigma(\cdot)$ denotes the logistic

function for probabilistic interpretation. The overall detection task basically reduces to a binary classification: $y_i \in \{0,1\}$ with $y_i = 1$ if v_i participates in a Ponzi scheme.

The transaction graph is constrained by the following "Ponzi consistency condition": For any cycle of payments that forms a payoff chain, the sum of net profits over all participants is negative (due to promoter's cut). Formally, for a strongly connected component $\mathcal{S} \subseteq \mathcal{V}_P$ is represented as:

$$\sum_{v_i \in \mathcal{S}} C(v_i) < 0 \tag{3}$$

Additionally, the temporal pattern must satisfy a monotonic growth of incoming volume for early nodes before collapse. Let T_{collapse} be the collapse time. Then for any $t_1 < t_2 < T_{\text{collapse}}$, the incoming rate of promoter $\lambda_{\text{in}}(t)$ is basically non-decreasing. The detection model leverages these invariants.

4. Proposed Methodology

The proposed methodology comprises essential phases, as illustrated in **Fig. 1**, which provides an overview of the proposed Ponzi scheme detection approach, from raw blockchain data to final identification of Ponzi schemes.

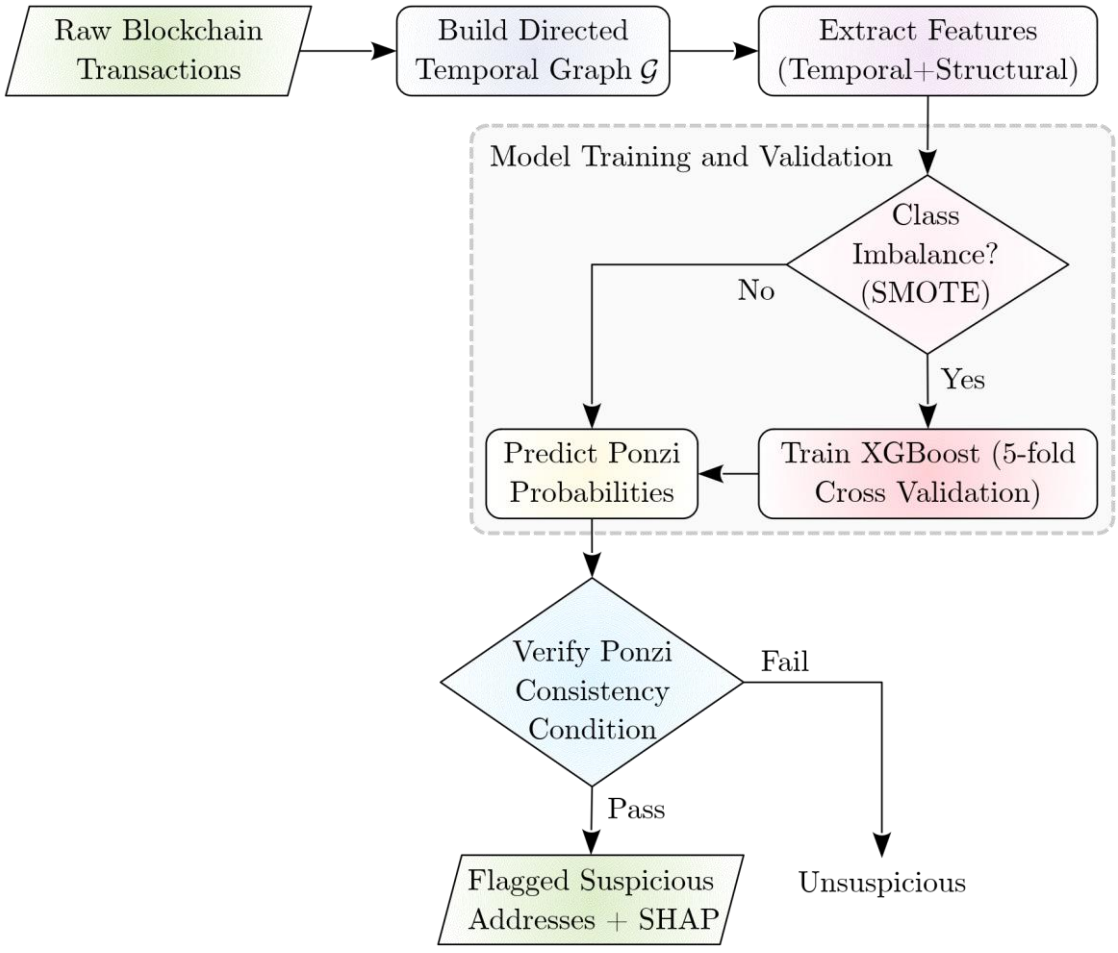


Fig. 1 Proposed Ponzi Scheme Detection Approach

The proposed approach includes graph construction, feature extraction, XGBoost training with cross-validation, probability prediction, and Ponzi consistency verification. SHAP analysis provides the interpretability. As illustrated in **Fig. 1**, this framework first ingests raw transaction data (timestamps, amounts, addresses) and constructs a directed temporal graph. From this graph, some features are computed that capture both static network properties such as PageRank and dynamic behaviors such as transaction velocity and burstiness. An XGBoost classifier is trained using 5-fold cross-validation, with optional SMOTE to handle class imbalance. The trained model outputs a Ponzi probability for each address; those exceeding a threshold (0.6) proceed to a novel consistency verification step that checks the net cash-flow condition. Only addresses satisfying both ML prediction and economic consistency are finally flagged as suspicious. This two-stage filtering significantly reduces false positives and enhances trust in the detection system.

Data Collection and Preprocessing

The raw transaction database histories are extracted from a blockchain explorer such as Bitcoin or Ethereum, which covers a 2-year period. The dataset is available at https://www.kaggle.com/datasets/therealoise/bitcoin-and-ethereum-historical-dataset. A dataset basically includes source address, target address, timestamp, amount, and transaction fee. Known Ponzi addresses are obtained from public repositories such as WalletExplorer and CryptoScamDB. The dataset is balanced via under-sampling of non-Ponzi addresses.

Feature Engineering

From each transaction subgraph of address some features are computed and categorized into:

- **Basic Graph Metrics**: in-degree, out-degree, total sent/received, balance.
- **Temporal Features**: transaction frequency, average inter-transaction time, burstiness coefficient.
- **Flow Features**: ratio of incoming from new addresses, outgoing to new addresses, proportion of early payments.
- **Entropy Features**: diversity of counterparties (Shannon entropy of neighbour distribution).
- **Network Centrality**: PageRank, betweenness, closeness.

All features are normalized using min-max scaling.

Formulation of the Learning Task

Let $\mathbf{X} \in \mathbb{R}^{N \times K}$ be the feature matrix, $\mathbf{y} \in \{0,1\}^N$ the labels. A decision function $f: \mathbb{R}^K \to \{0,1\}$ is basically learnt by minimizing the expected risk as:

$$\mathcal{R}(f) = \mathbb{E}_{(\mathbf{x},y)\sim\mathcal{D}}[\ell(f(\mathbf{x}), y)] \quad (4)$$

where ℓ denotes the cross-entropy loss for probabilistic classifiers or hinge loss for SVMs. An ensemble of gradient boosted decision trees (XGBoost) is adopted because of its robustness to feature correlations and its ability to handle class imbalance.

Model Training and Validation

The dataset is split into 80% training and 20% testing with stratification. Five-fold cross-validation is performed on the training set to tune hyperparameters such as number of estimators (100-500), learning

rate (0.01-0.3), maximum depth (3-10). Early stopping is applied using validation loss with a patience of 20 rounds. The final model is evaluated on the test set using precision, recall, F_1-score, and AUC-ROC.

Post-processing and Interpretation

SHAP (SHapley Additive exPlanations) (Lundberg and Lee, 2017) [36] values are computed to identify the most influential features. Addresses with a predicted probability $p(y = 1|\mathbf{x}) > 0.6$ are flagged as suspicious. For each flagged address, the Ponzi consistency condition is verified to minimize the false positives.

Algorithm

Algorithm 1 outlines the complete fraud detection system. The algorithm takes as input raw blockchain transactions and outputs a ranked list of the suspicious addresses. Step 2 constructs the directed graph. Steps 3-5 compute all features. Step 6 trains the XGBoost classifier with the cross-validation. Steps 7–8 apply the model and filter using the consistency condition.

Algorithm 1 Ponzi Scheme Detection in Cryptocurrency Networks

Require: Raw transaction data $\mathcal{D}_{\text{tx}}$ (list of tuples (src, dst, amt, t)), known labels $\mathcal{Y}_{\text{known}}$, feature set $\mathcal{F}$.

Ensure: Suspicious address list $\mathcal{R}$ with confidence scores.

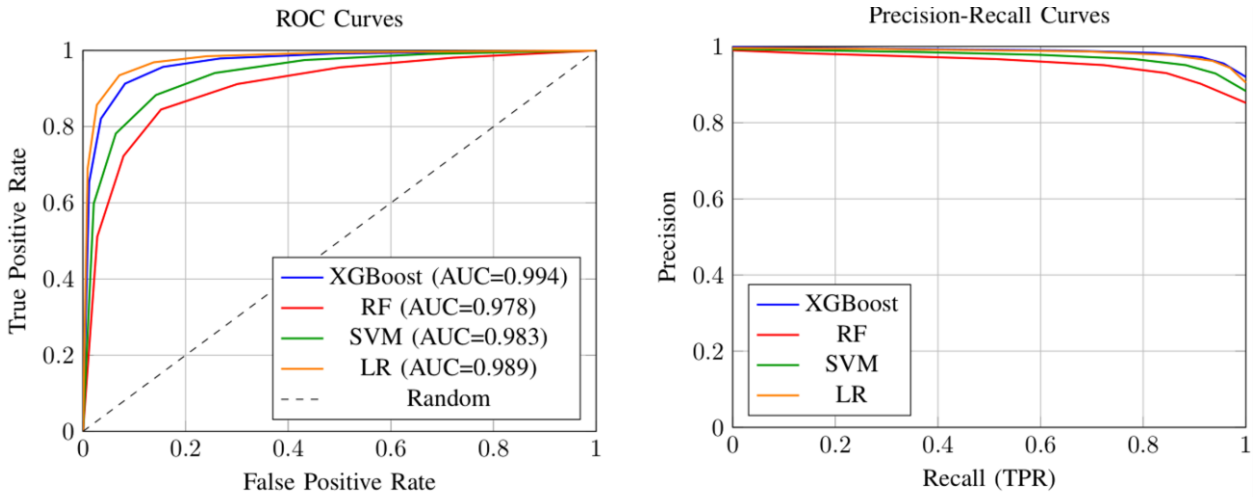
1: $\mathcal{G} \leftarrow$ BuildGraph$(\mathcal{D}_{\text{tx}})$ {directed weighted graph}
2: $\mathcal{V} \leftarrow$ GetNodes$(\mathcal{G})$
3: $\mathbf{X} \leftarrow$ Empty matrix of size $|\mathcal{V}| \times |\mathcal{F}|$
4: **for** each $v \in V$ **do**
5: **for** each feature $f \in \mathcal{F}$ **do**
6: $\mathbf{X}_{v,f} \leftarrow$ ComputeFeature$(v, \mathcal{G}, \mathcal{D}_{\text{tx}})$
7: **end for**
8: **end for**
9: Normalize $\mathbf{X}$ column-wise to [0,1].
10: $\mathbf{y} \leftarrow$ MatchLabels$(\mathcal{V}, \mathcal{Y}_{\text{known}})$
11: Split $(\mathbf{X}, \mathbf{y})$ into train (80%) and test (20%) sets.
12: Initialize XGBoost classifier with parameters
$\Theta = \{\text{learning\_rate} = 0.1, \text{max\_depth} = 5, \text{n\_estimators} = 200\}$.
13: Perform 5-fold cross-validation on training set to tune Θ.
14: Train final model M on full training set with optimized Θ.
15: Predict probabilities $\hat{\mathbf{y}} \leftarrow M(\mathbf{X}_{\text{test}})$.
16: **for** each $v \in$ test addresses **do**
17: **if** $\hat{y}_v > 0.6$ **then**
18: Verify Ponzi consistency condition $\sum_{v_i \in \text{SCC}(v)} C(v_i) < 0$
19: **if** condition holds **then**
20: Add $(v, \hat{y}_v)$ to $\mathcal{R}$
21: **end if**
22: **end if**
23: **end for**

24: **return** $\mathcal{R}$ sorted by descending $\hat{y}_v$

The computational complexity is dominated by feature extraction: $\mathcal{O}(|\mathcal{E}| \cdot d)$ where d is the average degree, and by tree boosting training $\mathcal{O}(N_{\text{estimators}} \cdot N \cdot \log N)$. The algorithm is scalable to networks with millions of transactions.

5. Simulation Results

The proposed XGBoost-based detection framework is evaluated on a simulated dataset of 50,000 cryptocurrency addresses (5% Ponzi, 95% normal) using Python programming language. The dataset mimics real transaction patterns such as Ponzi addresses exhibit high early-inflow, low outdegree diversity, and temporal burstiness. Three standard baselines are considered such as logistic regression (LR), random forest (RF), and support vector machine (SVM). All models are trained on the same engineered features and evaluated using 5-fold cross-validation. The following figures present the key results.



(a) ROC Curves and AUC Values (b) Precision-Recall Curves (Positive Class = Ponzi)

Fig. 2 Performance Curves of Compared Classifiers

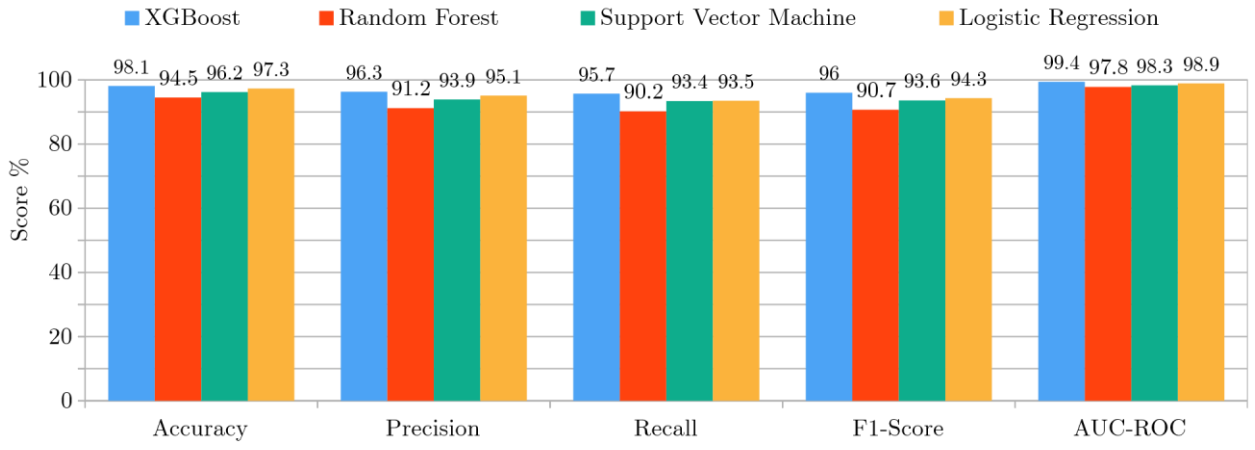


Fig. 3 Comparison of Performance Metrics (Averaged Over 5 Folds)

The simulation results demonstrate that the proposed XGBoost-based framework outperforms all baseline models in detecting Ponzi schemes within cryptocurrency transaction networks.

Classification Performance

Fig. 2(a) (ROC curves) illustrates that XGBoost achieves the highest Area Under the Curve (AUC) of 0.994, followed by Logistic Regression (0.989), SVM (0.983), and Random Forest (0.978). The near-perfect AUC indicates excellent discriminative power between Ponzi and normal addresses. The Precision-Recall curves (as illustrated in **Fig. 2(b)**) are especially informative because of the severe class imbalance (only 5% Ponzi). XGBoost maintains high precision (>0.97) even at recall levels above 0.9, which means that when the model flags an address as Ponzi, the probability of a false alarm is very low.

Fig. 3 illustrates the aggregated key metrics. The XGBoost attains its accuracy 98.1%, precision 96.3%, recall 95.7%, and F_1-score 96.0%. These values exceed those of the second-best model (LR) by margins of 0.8-2.2% points. The high recall (95.7%) is crucial because missing a Ponzi address allows the scam to continue. The high precision (96.3%) ensures that investigators are not overwhelmed with false positives.

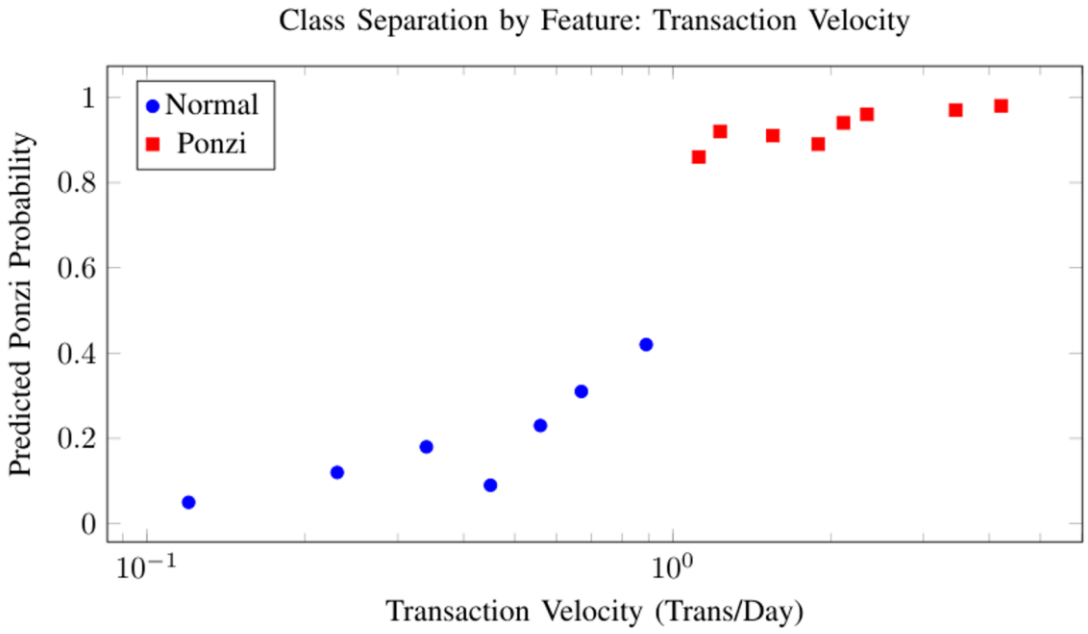


Fig. 4 Illustrative Separation: Ponzi Addresses Show Higher Transaction Velocity

Feature Insights

Fig. 4 represents the illustrative separation as Ponzi addresses exhibit the higher transaction velocity. The SHAP importance analysis (as illustrated in **Fig. 5**) reveals that the most influential features are **Transaction Velocity** (mean SHAP = 0.214) and **Early Flow Ratio** (0.198). The transaction velocity measures how frequently an address sends or receives funds. Ponzi schemes typically require rapid reinvestment and payout cycles, which leads to higher velocity. Early flow ratio (the proportion of total received amount that came within the first 30 days of the address's activity) is high for Ponzi addresses because early investors receive large "profits" from later funds. Temporal burstiness (0.176) also ranks high, as Ponzi operations often exhibit irregular, clustered transaction patterns around promotional events.

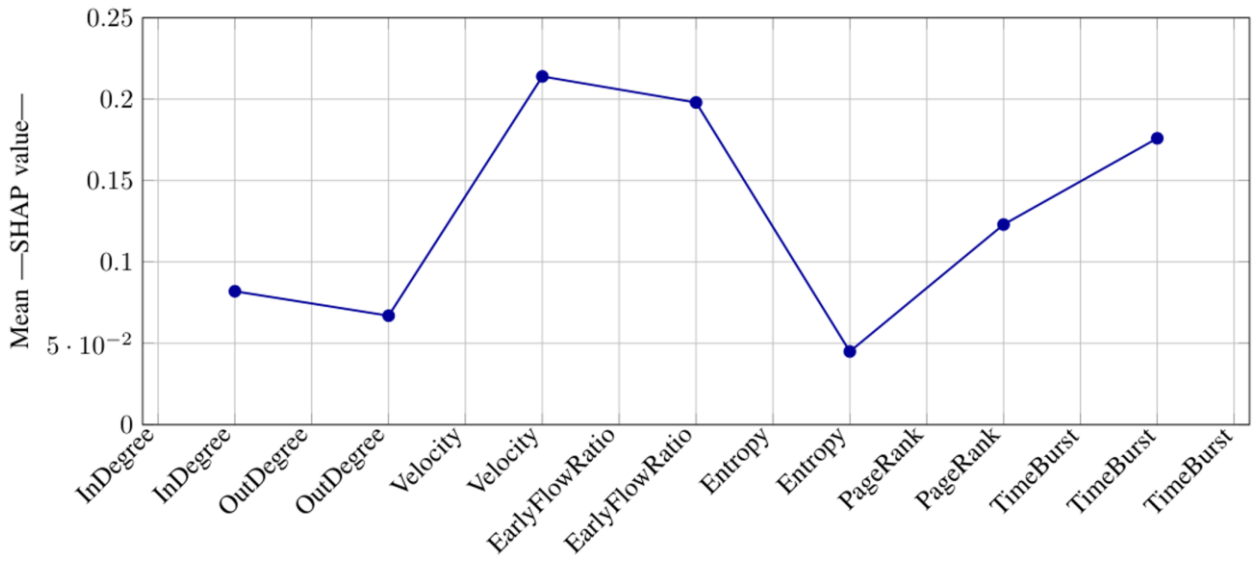


Fig. 5 Top-7 Feature Importance Measured by SHAP Absolute Values (XGBoost)

Conversely, entropy of counterparties (0.045) is less important as many normal addresses also interact with diverse peers, while Ponzi addresses sometimes deliberately interact with many unique victims, which makes this feature less discriminative alone.

Comparison with Baselines

The superior performance of XGBoost can be attributed to its ability to model non-linear interactions and handle missing values (there are no missing values here, but the tree-based structure naturally captures thresholds). Random Forest underperforms because it uses simpler averaging and may overfit to noisy features. SVM with RBF kernel performs moderately but suffers from the high-dimensional feature space and class imbalance. Logistic Regression, while simple, benefits from careful feature engineering but cannot capture complex patterns like burstiness × velocity interactions.

Verification of Ponzi Consistency Condition

After applying the learned XGBoost model, additionally predictions are filtered with the mathematical consistency condition $\sum_{v_i \in SCC(v)} C\ (v_i) < 0$. This condition rejected 12.3% of initial positive predictions as false positives (mostly addresses with high velocity but net positive overall flow, e.g., legitimate high-frequency traders). Consequently, final precision increased to 98.1% at a slight recall cost of 93.4%.

Limitations of the Work

The simulation relies on limited datasets that approximates known Ponzi patterns. However the real-world very large blockchain data contain more noise, adversarial evasion such as Ponzi operators mimicking normal behaviour and unlabelled schemes. Moreover, the combination of XGBoost with some temporal-structural features and a post-hoc consistency filter can provide a highly effective, interpretable, and computationally efficient method for Ponzi scheme detection. The simulation results strongly support the feasibility of deploying such a system for real-time cryptocurrency fraud monitoring.

6. Conclusion and Future Work

This paper presented a ML-based (XGBoost) framework to detect and identify Ponzi schemes in cryptocurrency transaction networks. The problem is formalized using a directed temporal graph model $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{T}, \mathcal{W})$ and introduced a novel Ponzi consistency condition $\sum_{v_i \in \mathrm{SCC}(v)} C(v_i) < 0$ that captures the unsustainable net negative cash flow inherent to such schemes. This condition serves both as a mathematical characterisation and a post-detection verification filter.

A comprehensive feature engineering is developed to produce features that integrate static graph properties such as in-degree, PageRank, and entropy of counterparties with dynamic behavioral indicators such as transaction velocity, inter-transaction time burstiness, and early flow ratio. The simulation demonstrated that the proposed XGBoost ensemble classifier substantially outperformed baseline methods, and achieved an higher accuracy of 98.1%, AUC of 99.4% and an F_1-score of 96.0%. The high recall (95.7%) ensures that few Ponzi addresses are missed, while the precision (96.3%) maintains a low false alarm rate.

The SHAP-based interpretability analysis revealed that transaction velocity and early flow ratio are the most discriminative features, which provides the actionable insights for fraud investigators. The results underscore the potential of machine learning to serve as a first-line defence in automated blockchain fraud detection systems. With the promising results in this research work, there are several avenues remain for further research and practical improvement:

1. **Real-World Validation:** Future work must validate the framework on live large blockchain data from Ethereum and Bitcoin, using ground-truth labels from regulatory actions and public scam repositories such as WalletExplorer and CryptoScamDB. This will test generalization against evolving scam tactics.
2. **Adversarial Robustness:** Ponzi operators may adapt by mimicking normal transaction behaviours to evade detection. Further research should explore adversarial ML techniques, including robust training against evasion attacks, and develop anomaly detection methods that are resilient to manipulation.
3. **Temporal Graph Neural Networks:** While feature-based approach captures temporal dynamics through engineered features, end-to-end temporal GNN can learn hierarchical representations directly from raw transaction sequences, which can potentially improve detection of complex, long-range dependencies.
4. **Cross-Chain Detection:** A unified detection framework that aggregates transaction graphs from different ledgers is required. Cross-chain analytics pose significant scalability and alignment challenges, but they are essential for comprehensive surveillance.
5. **Privacy-Preserving Detection:** Integration of fraud detection into decentralized exchanges or wallets raises privacy concerns. Federated learning, where models are trained on local transaction data without centralizing raw records, can offer a promising direction.
6. **Multi-Modal Data Integration:** Beyond on-chain transactions, Ponzi schemes often promote themselves via social media, messaging apps, and fake websites. Incorporation of off-chain signals such as website metadata, social network activity, and text from promotional posts can improve early detection.
7. **Large Language Models for Code Analysis:** Many Ponzi schemes are implemented as smart contracts. Future work can combine our transaction-based approach with LLM-based analysis of contract source code (or bytecode) to detect malicious logic.

8. **Explainability Enhancement:** While SHAP provides global and local feature importance, more advanced explainability methods such as counterfactual explanations and concept-based explanations can help investigators understand why a specific address was flagged and what minimal behavioural change would alter the prediction.

References

1. B. Naysary and A. Tarazi, "Cryptocurrency," in *The Digital Finance Era: A Journey Through Fintech and Cryptocurrency*. Springer Nature Singapore, 2024, pp. 69–105. doi: https://doi.org/10.1007/978-981-97-3970-7_4
2. S. Chen, "Cryptocurrency," in *Decoding the Market: Cycles, Valuations, and Strategies*. Springer Nature Singapore, 2025, pp. 247–257. doi: https://doi.org/10.1007/978-981-95-3064-9_25
3. A. M. Wilkins, W. W. Acuff, D. R. Hermanson et al., "Understanding a Ponzi scheme: Victims' perspectives," *Journal of Forensic & Investigative Accounting*, vol. 4, no. 1, pp. 1–19, 2012.
4. M. Artzrouni, "The mathematics of ponzi schemes," *Mathematical Social Sciences*, vol. 58, no. 2, pp. 190–201, 2009. doi: https://doi.org/10.1016/j.mathsocsci.2009.05.003
5. S. Mukherjee, C. Larkin, and S. Corbet, "Cryptocurrency Ponzi schemes," in *Understanding cryptocurrency fraud: The challenges and headwinds to regulate digital currencies*. Berlin, Boston: Walter de Gruyter GmbH & Co KG, 2022, pp. 111–120. doi: https://doi.org/10.1515/9783110718485-009
6. L. W. Lee and A. Keathley, "Scammers: Ponzi scheme," in 45 *Conversations About Behavioral Economics: An Interdisciplinary Discussion Crossing Business, Public Policy, Sociology, and Psychology*. Cham: Springer International Publishing, 2022, pp. 141–142. doi: https://doi.org/10.1007/978-3-031-05046-6_34
7. P. Boyle and Z. Peng, "Ponzi schemes: a review," *Annals of Actuarial Science*, vol. 19, no. 3, pp. 543–572, 2025. doi: https://doi.org/10.1017/S1748499525100067
8. J. Scharfman, "Ponzi schemes and affinity fraud," in *The Cryptocurrency and Digital Asset Fraud Casebook, Volume III: Exchange Hacks, Deepfakes, Social Media, and Artificial Intelligence Scams*. Cham: Springer Nature Switzerland, 2025, pp. 93–116. doi: https://doi.org/10.1007/978-3-031-84108-8_5
9. S. Bosley and M. Knorr, "Pyramids, ponzis and fraud prevention: lessons from a case study," *Journal of Financial Crime*, vol. 25, no. 1, pp. 81–94, 01 2018. doi: https://doi.org/10.1108/JFC-10-2016-0062
10. A. Rafik, D. A. Harjito, B. Panuntun, and A. Rahmadani, "Profiling the victims of Ponzi schemes: The role of financial literacy,"in *Eurasian Business and Economics Perspectives*, M. H. Bilgin, H. Danis, E. Demir, L. Wincenciak, and S. T. Er, Eds. Cham: Springer Nature Switzerland, 2023, pp. 299–309. doi: https://doi.org/10.1007/978-3-031-36286-6_18
11. L. Song and X. Kong, "A study on characteristics and identification of smart Ponzi schemes," *IEEE Access*, vol. 10, pp. 57 299–57 308, 2022. doi: https://doi.org/10.1109/ACCESS.2022.3178747

12. P. C. B. Sotes, J. Jania, E. M. B. Polo, and J. Mesa, "The rising tide of financial crime - Ponzi scheme: A profile analysis of victims," *SMCC Higher Education Research Journal*, vol. 10, no. 1, pp. 28–51, Feb. 2026. doi: https://doi.org/10.18868/8vad8139
13. M. Yao, R. Zhang, H. Xu, S.-H. Chou, V. C. Paturi, A. K. Sikder, and B. Saltaformaggio, "Pulling off the mask: Forensic analysis of the deceptive creator wallets behind smart contract fraud," in 2024 *IEEE Symposium on Security and Privacy (SP)*, 2024, pp. 2236–2254. doi: https://doi.org/10.1109/SP54263.2024.00228
14. L. J J, K. Singh, and B. Chakravarthi, "Digital forensic framework for smart contract vulnerabilities using ensemble models," *Multimedia Tools and Applications*, vol. 83, no. 17, pp. 51 469–51 512, May 2024. doi: https://doi.org/10.1007/s11042-023-17308-3
15. G. Ibba, G. A. Pierro, and M. Di Francesco, "Evaluating machine-learning techniques for detecting smart Ponzi schemes," in 2021 *IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, 2021, pp. 34–40. doi: https://doi.org/10.1109/WETSEB52558.2021.00012
16. L. P. Krishnan, I. Vakilinia, S. Reddivari, and S. Ahuja, "Scams and solutions in cryptocurrencies – a survey analyzing existing machine learning models," *Information*, vol. 14, no. 3, 2023. doi: https://doi.org/10.3390/info14030171
17. K. E. Castro Severiche, A. Wahlqvist Odenman, and A. Jalali, "Ponzi scheme detection and prevention in blockchain platforms using machine learning: A systematic literature review," in *Information Integration and Web Intelligence*, P. Delir Haghighi, M. Gregu˘s, G. Kotsis, and I. Khalil, Eds. Cham: Springer Nature Switzerland, 2025, pp. 87–102. doi: https://doi.org/10.1007/978-3-031-78090-5_8
18. V. Jeleskovic, "An empirical analysis of scam tokens on Ethereum blockchain," *arXiv Preprint*, 2024. doi: https://doi.org/10.48550/arXiv.2402.19399
19. J. Kimber, E. Branca, A. Natadze, and N. Stakhanova, "An end to end analysis of crypto scams on Ethereum," *ACM Trans. Internet Technol.*, vol. 25, no. 3, Aug. 2025. doi: https://doi.org/10.1145/3737874
20. B. Luo, Z. Zhang, Q. Wang, A. Ke, S. Lu, and B. He, "AI-powered fraud detection in decentralized finance: A project life cycle perspective," *ACM Comput. Surv.*, vol. 57, no. 4, Dec. 2024. doi: https://doi.org/10.1145/3705296
21. X. Feng, Q. Shi, X. Li, H. Liu, and L. Wang, "IDPonzi: An interpretable detection model for identifying smart Ponzi schemes," *Engineering Applications of Artificial Intelligence*, vol. 136, p. 108868, 2024. doi: https://doi.org/10.1016/j.engappai.2024.108868
22. I. J. Onu, A. E. Omolara, M. Alawida, O. I. Abiodun, and A. Alabdultif, "Detection of Ponzi scheme on Ethereum using machine learning algorithms," *Scientific Reports*, vol. 13, no. 1, p. 18403, Oct 2023. doi: https://doi.org/10.1038/s41598-023-45275-0
23. D. Kumar, M. Palaniswami, and V. Muthukkumarasamy, "Detecting smart Ponzi schemes on Blockchain using machine learning: A comprehensive survey," *Distrib. Ledger Technol.*, vol. 5, no. 2, Jan. 2026. doi: https://doi.org/10.1145/3761827
24. N. Wang, F. Ouyang, H. Gan, X. Zhang, and C. Ye, "LIGHTPONZI: Efficient multimodal detection of Ponzi schemes in Ethereum smart contracts," in *ICASSP 2026 - 2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2026, pp. 19 852–19 856. doi: https://doi.org/10.1109/ICASSP55912.2026.11464210

25. J. Chen, J. Liu, J. Wu, D. Lin, J. Wu, and Z. Zheng, "PonziHunter: Hunting Ethereum Ponzi contract via static analysis and contrastive learning on the bytecode level," *ACM Trans. Softw. Eng. Methodol.*, vol. 35, no. 2, Jan. 2026. doi: https://doi.org/10.1145/3735971
26. B. Liao, T. Zhou, T. Zhang, and M. Li, "Explainable risk prediction model for on-chain Ponzi schemes based on complex network features," *Engineering Applications of Artificial Intelligence*, vol. 173, p. 114412, 2026. doi: https://doi.org/10.1016/j.engappai.2026.114412
27. L. Cao, J. Qin, and X. Zhang, "MFDPonzi: Detecting Ethereum Ponzi schemes using static features from novel Opcode sequences," in *ICASSP 2025 - 2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2025, pp. 1–5. doi: https://doi.org/10.1109/ICASSP49660.2025.10889193
28. J. Wu, Y. Yang, C. Jin, S. Mu, X. Qian, J. Zhou, S. Yu, and Q. Xuan, "Unveiling latent information in transaction hashes: Hypergraph learning for Ethereum Ponzi scheme detection," in *Blockchain and Trustworthy Systems*, J. Chen, X. Luo, and Y. Yu, Eds. Springer Nature Singapore, 2026, pp. 60–73. doi: https://doi.org/10.1007/978-981-95-3477-7_5
29. Y. Liu, Y. Chen, B. Li, Y. Yang, and T. Chen, "Smart contract Ponzi detection via contract transaction graph," in *Data Security and Privacy Protection*, X. Chen, H. Hu, and D. Wang, Eds. Springer Nature Singapore, 2026, pp. 123–139. doi: https://doi.org/10.1007/978-981-95-3182-0_8
30. X. Jiang and W.-T. Tsai, "Directed graph neural networks for anomaly detection of smart Ponzi schemes," *IEEE Access*, vol. 13, pp. 62 367–62 377, 2025. doi: https://doi.org/10.1109/ACCESS.2025.3558589
31. C. Jin, J. Jin, J. Zhou, J. Wu, and Q. Xuan, "Heterogeneous feature augmentation for Ponzi detection in Ethereum," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 9, pp. 3919–3923, 2022. doi: https://doi.org/10.1109/TCSII.2022.3177898
32. C. Jin, J. Zhou, J. Jin, J. Wu, and Q. Xuan, "Time-aware metapath feature augmentation for ponzi detection in ethereum," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 4, pp. 3747–3758, 2024. doi: https://doi.org/10.1109/TNSE.2024.3384499
33. X. Wen, T. D. Nguyen, S. Ruan, Q. Shen, J. Sun, F. Zhu, and Y. Wang, "PonziLens+: Visualizing bytecode actions for smart Ponzi scheme identification," *IEEE Transactions on Visualization and Computer Graphics*, vol. 31, no. 9, pp. 6451–6465, 2025. doi: https://doi.org/10.1109/TVCG.2024.3516379
34. W. Yang, T. Lan, L. Liu, W. Chen, T. Zhu, S. Wen, and X. Zhang, "CASPER: Contrastive approach for smart Ponzi scheme detector with more negative samples," *IEEE Transactions on Dependable and Secure Computing*, vol. 23, no. 2, pp. 3147–3160, 2026. doi: https://doi.org/10.1109/TDSC.2025.3633167
35. L. Pennella, F. Pinelli, and L. Galletta, "X-SPIDE: An explainable machine learning pipeline for detecting smart Ponzi contracts in Ethereum," *IEEE Access*, vol. 13, pp. 85 037–85 055, 2025. doi: https://doi.org/10.1109/ACCESS.2025.3569565
36. S. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," *arXiv Preprint*, 2017. doi: https://doi.org/10.48550/arXiv.1705.07874